associating each raw event with one or more rules that correspond with a type parameter of the raw event; and

applying each rule to its associated group of raw events; and

determining if a computer attack or security breach has occurred based upon successful application of a rule.

14. (Once Amended) A method for determining relationships between two or more computer events, comprising the steps of:

receiving a plurality of raw events having a first set of parameters;

creating raw event storage areas based upon information received from a raw event classification database;

storing each event in an event storage area based upon an event type parameter;

comparing each raw event to data contained in a context database;

adjusting a priority parameter or leaving the priority parameter in tact for each raw event in response to the comparison to the context database;

associating each raw event with one or more correlation events ;

applying one or more rules to each event based upon the correlation event associations; and

generating a mature correlation event message in response to each successful application of a rule.

16. (Once Amended) The method of claim 14, wherein the context database comprises any one of vulnerability values, computer event frequency values, source and destination zone values, and detector zone values.

17. (Once Amended) The method of claim 14, wherein the raw event classification database comprises tables that include information that categorizes raw events based on any one of the following: how an activity indicated by a raw event may impact one or more target computers, how many target computers may be affected by an activity indicated by a

A5

raw event, and how activities indicated by respective raw events gain access to one or more target computers.

24. (Once Amended) The fusion engine of claim 22, wherein the context database comprises any one of vulnerability values, computer event frequency values, source and destination zone values, and detector zone values.

A6

25. (Once Amended) The fusion engine of claim 22, wherein the raw event classification database comprises tables that include information that categorizes raw events based on any one of the following: how an activity indicated by a raw event may impact one or more target computers, how many target computers may be affected by an activity indicated by a raw event, and how activities indicated by respective raw events gain access to one or more target computers.

Please Add the following additional claims:

26. (Newly Added) A method for managing security information comprising the steps of:

receiving a raw event having a first ranking from one or more data sources;

classifying the raw event;

storing the raw event; and

A7

assigning a second ranking to the raw event, whereby the second ranking assesses risks of the raw event based upon a context of the raw event.

27. (Newly Added) The method of claim 26, wherein the first ranking comprises one or more relative values measuring potential risk or damage that is associated with an activity indicated by the raw event.

28. (Newly Added) The method of claim 26, wherein the step of assigning a second ranking to each raw event further comprises the steps of:

comparing parameters of each raw event with information in a database; and

assigning additional parameters to each raw event relating to the environment of the raw event.

29. (Newly Added) The method of claim 28, wherein the additional parameters comprise at least one of a priority status, a vulnerability status, a historical frequency value, a source zone value, a destination zone value, a detector zone value, and a priority change reason text string.

30. (Newly Added) The method of claim 26, wherein the step of assigning a second ranking to each raw event further comprises the steps of:

identifying a priority status parameter of a raw event;

comparing each raw event to information contained in a context database;

changing the priority status parameter of a respective raw event if a match occurs in response to the comparison step; and

leaving the priority status in tact if a match does not occur in response to the comparison step.

31. (Newly Added) A method for managing security information comprising the steps of:

receiving raw events from one or more data sources;

classifying the raw events;

grouping two or more raw events into a high level correlation event;

in response to grouping the two or more raw events, generating a mature correlation event message; and

displaying one or more mature correlation event messages on a console that describe relationships between raw events, whereby a number of events displayed on the console can be substantially minimized.

32. (Newly Added) The method of claim 31, wherein each raw event comprises suspicious computer activity detected by one of an automated system and human observation.

33. (Newly Added) The method of claim 31, wherein the step of receiving raw events from one or more data sources further comprises the step of receiving real-time raw events from one of intrusion detection system, a detector within an intrusion detection system, and a firewall.

34. (Newly Added) The method of claim 31, wherein the step of receiving raw events from one or more data sources further comprises the step of receiving raw events from one of a file and database.

35. (Newly Added) The method of claim 31, wherein the step of classifying the raw events further comprises the steps of:

identifying an event type parameter for each raw event;

comparing the event type parameter with an event type category of a list; and

assigning each raw event to a corresponding event type category in the list.

36. (Newly Added) The method of claim 31, wherein the step of classifying comprises the step of categorizing a raw event based on any one of the following: how an activity indicated by a raw event may impact one or more target computers, how many target computers may be affected by an activity indicated by a raw event, and how activities indicated by respective raw events gain access to one or more target computers.

37. (Newly Added) The method of claim 31, wherein the step of grouping two or more raw events further comprises the step of determining a time at which a respective raw event occurred relative to another raw event.